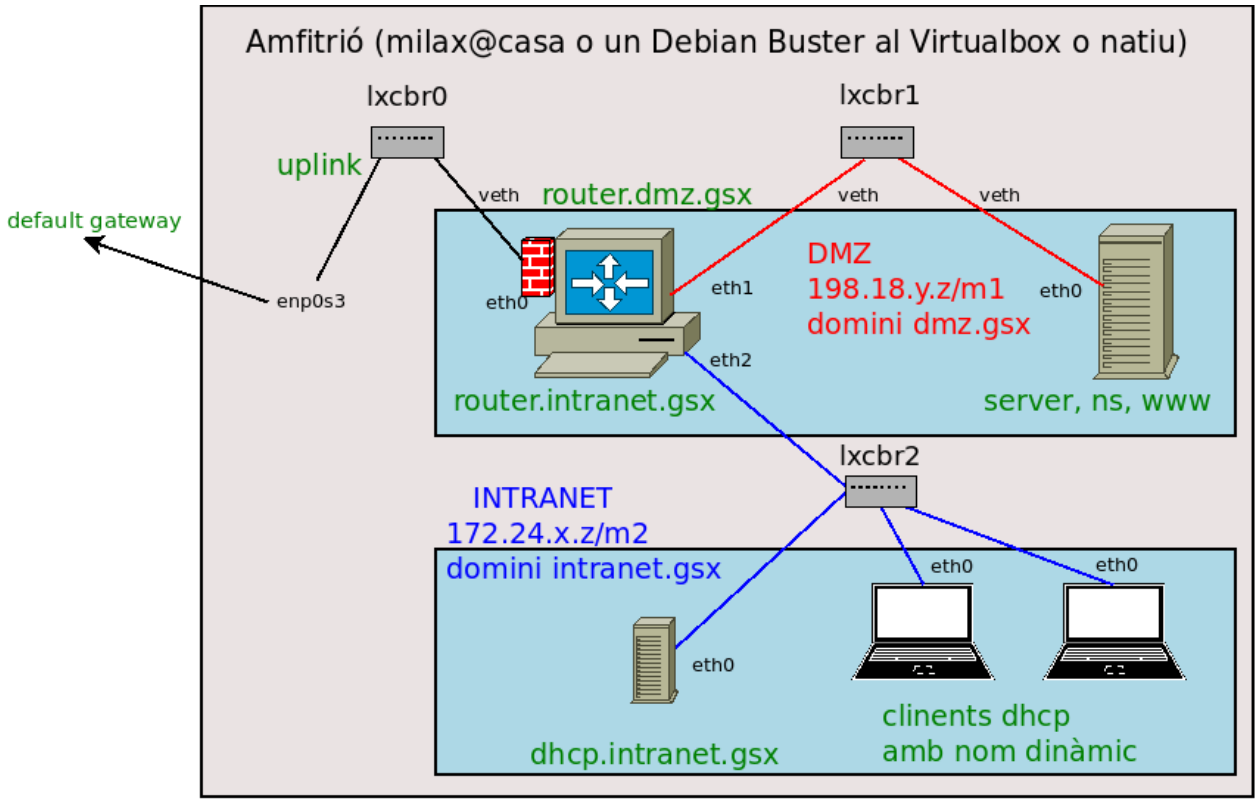
Pràctica 3, part 2: Servei DNS

Què farem:

- Partirem del laboratori anterior funcionant: el router activat, el dhcp funcionant, els clients aturats.
- Configurarem un servidor DNS al contenidor anomenat **server**.
- Adequarem la configuració del servidor DHCP per a que proporcioni als seus clients la informació del nou servei.
- Als contenidors configurats estàticament haurem de modificar els seu resolver.

A la topologia podeu trobar els noms (en color verd) que usarà cada contenidor:



A tots els contenidors:

Com ara ja disposarem de servei DNS ja no cal modificar el fitxer /etc/hosts. Les màquines posades als laboratoris anteriors les haureu de treure per a no interferir en les proves del DNS. Als *scripts* comenteu les línies que el modificaven.

0) Al router: executem l'script labx1_config_router.sh per atenir connectivitat al server.

A) Al contenidor 'server': hi posarem el servei de noms DNS

- Modifiquem temporalment el fitxer /etc/resolv.conf posant-hi com a nameserver un de genèric, com ara el de google o el de cloudfare (one.one.one.one).
- Comprovem que tenim els paquets **bind9**, **bind9-doc** i **dnsutils** i, si cal, els instal·lem.
- Un cop instal·lats, copiarem els fitxers de **/etc/bind/named*** al directori local per a poder-los editar manualment.
- Configurem els servidor DNS[1]:
  - Editeu el fitxer ./**named.conf.options**, posant-hi:
    - Especifiqueu que el directori de fitxers per defecte sigui a **/var/cache/bind/** (per a poder escriure a la part3).
    - el **forwarding** les consultes desconegudes cap al servidor DNS del ISP (el que tingui configurat el router)[2]. Per exemple:

```
ssh router "grep \"^nameserver\" /etc/resolv.conf"
```

      Aquests dns no els validarem: desactiveu la validació **dnssec**.
    - **queries recursius** permesos només per als nostres contenidors: useu una acl.
    - **transferències de zona** sols permeses des del localhost.
    - Resta d'opcions:

```
auth-nxdomain no;
dnssec-validation no;
listen-on-v6 { none; };
```

  - Editeu el fitxer ./**named.conf.local** :
    - Hi afegim **dues** zones, per als dominis **intranet.gsx** i **dmz.gsx**.
    - Hi afegim **dues** zones inverses.
      - Tingueu en compta que a la Intranet usem una classe B (2 bytes per a la zona, 2 bytes per als RR).

      → els noms dels fitxers amb les dades han d'incloure el path **/etc/bind/**

1 *Us podeu basar en l'exemple Ex1 de les transparències de teoria (servidor autoritari).*

2 *Si teniu un virtualbox hi heu aplicat el .bat proporcionat llavors serà el del virtualbox: 10.0.2.3*

  - Modifiquem el fitxer **/etc/default/named** per a que als paràmetres d'inici sols atengui peticions IPv4 (-4).

- Editem els **fitxers de zona (*forward*)**:
  - Cada zona ha de definir un RR NS amb la IP que té el propi servidor DNS.
  - Afegiu tots els noms que apareixen a la figura de la topologia (color verd).
  - Afegiu registres **CNAME** duplicats del ns (server i www).
  - Com el DNS no té IP a la intranet, llavors a la zona **intranet.gsx** hi haurem de posar com a NS la IP del servidor de noms però de la DMZ !
- Editem els **fitxers de zona inversa (*reverse*):**
  - Hi posem els RRs inversos (apreu atenció amb el nombre de bytes)
  - Comprovem que per a cada entrada del fitxer de zona *forward* hi ha la corresponent entrada inversa.
- Comprovem les sintaxis de tots els .conf i els 4 fitxers de zona amb:

```
/sbin/named-checkconf -z $localdir/named.localconf
/sbin/named-checkzone 'NomZona' $localdir/fitxer_zona
```

  Aquest pas és important per a minimitzar el temps que el servei estigui inactiu *(downtime)*.
- Quan no hi hagi errors de sintaxi ja els podrem copiar a lloc:
  - Canviarem les propietats amb les que tenen els fitxers originals:

```
chmod/own --reference=/etc/bind/.....
```

  - Copiarem tots els fitxers named* a **/etc/bind/**
  - Copiarem els fitxers de zona a **/var/cache/bind/**
- Engeguem el servei com a *daemon*, i mirem el **journalctl** que tot segueixi correcte.[3]
- Modifiquem el fitxer /etc/resodlv.conf posant-hi com a nameserver el localhost i el search dels nostres dominis.
- *L'script* de configuració haurà de fer les instruccions que estan en **blau**.

B) Al contenidor 'router' com a client del DNS local:

- El router obté la configuració del /etc/**resolv.conf** del servidor dhcp extern i no usaria el nostre servidor DNS. Per això cal configurar el seu **client dhcp** per a

3 *En un entorn operatiu, hauríem de configurar canals de logging i categories, modificant el nivell de debug amb* `rndc trace`*. Vegeu un resum.*

que prefereixi primer (**prepend**) el nostre servidor de noms i els nostres dominis (**supersede**).

- Per seguretat volem que els nostres contenidors sols puguin consultar al nostre DNS. Per això afegiu una regla **iptables** que filtri a la cadena FORWARD totes les consultes DNS que surtin cap a Internet i que no vinguin del nostre server per a que els descarti.
- Apliqueu una DNAT inversa a la que vam fer a la sessió anterior: redirigiu tots els queries DNS que arribin a la eth0 del router redirigint-los cap al server.
- Executeu l'script i comproveu que el contingut del resolv.conf sigui correcte.

C) Al contenidor 'dhcp': servei DHCP

- Afegiu als fitxers locals adients el nostre domini a la opció ***domain-name,*** la IP del nostre DNS a la opció ***domain-name-servers*** i la opció ***domain-search*** per a que es pugui buscar noms dels 2 dominis.
- Modifiquem el fitxer /etc/resolv.conf posant-hi com a nameserver el server i el search dels nostres dominis.
- Executeu l'script i coomproveu l'estat del servei.

D) Als contenidors 'client':

- Cal assegurar que al fitxer **/etc/dhcp/dhclient.conf** faci el **request** dels domain-name i del domain-name-servers (sinó hi són, poseu-los al require).
- Abaixeu la eth0 i aixequeu-la.
- Comproveu visualment que el contingut del **resolv.conf** sigui correcte: ha de contenir com a *nameserver* només la IP del router i també el *search* dels dos dominis.
- Proveu:

```
ping ns
```

Proves:

- Comproveu amb les eines habituals (*dig, nslookup, host, resolvctl*) que des de tres màquines diferents (des del router, de la intranet i de la DMZ) que es serveixen:
  - les consultes directes a totes les zones.
  - les consultes inversos a totes les zones.
  - Fem pings extrem a extrem usant els diversos noms.

- Fem dues transferències de zona des del server. Exemple:

```
dig dmz.gsx AXFR
host -t AXFR intranet.gsx
```

- Intentem una transferència de zona des d'un client o del router (han de fallar).
- Provem un *query* des de fora (milax@casa o un pc a la xarxa de docència). Exemple:

```
milax@d200~# dig @IP_EXTERNA_ROUTER www.dmz.gsx
```

- Intentem un *query* recursiu des de fora (milax@casa o un pc a la xarxa de docència). Exemple:

```
milax@d200~# dig @IP_EXTERNA_ROUTER +recurse tinet.cat
```

Per a depurar problemes:

- Si el servei (bind) no es pot executar mirem el journal però del procés (named):

```
journalctl -u named -e
```

- Altrament, podem depurar les consultes:

```
rndc querylog
```

  i en un altre terminal (**lxc-attach**) del server capturem els logs permanentment:

```
journalctl -f
```

- Per contra, si volguéssim filtrar només de la darrera execució del servei podríem fer:

```
journalctl _PID=$(ps -C named -o pid=)
```

  Aquí hauríeu de poder veure les zones 'loaded' : les vostres i les *empty*.
- Si cal, proveu de capturar les consultes amb amb el wireshark/**tcpdump**.
- També podria ser necessari usar **dhcpdump**.

Documentació específica:

- man de named , named.conf i rndc
- Errors comuns (RFC1912.txt, informatiu)